Elektron Təhlükəsizlik Mərkəzi

Qaynar xətt: 1654
Email: reports@cert.az
Ünvan: Azərbaycan, Bakı, Droqal döngəsi, 702-ci məhəllə

Ziyanverici proqramlar

Ziyanverici proqramlar - informasiya sistemlərinə ziyan vurmaq üçün yaradılmış təhlükəli proqramlardır. Ziyanverici proqramlar sistemlərə istifadəçinin xəbəri və icazəsi olmadan yüklənir və kompüterin fəaliyyətinə təsir göstərir.

Ziyanverici proqramların daha geniş yayılmış növləri - troyanlar, casus proqramları, soxulcanlar, viruslar və şəbəkə qurdlarıdır.

- **Troyan** - xüsusilə yoluxduğu kompüterdən məlumatların toplanması, onların dəyişdirilməsi, kompüterin bədniyyətlinin nəzarətinə keçməsi və toplanmış məlumatları nəzarəti altında olduğu tərəfə ötürməsi ilə səciyyələnən ziyanverici proqramdır. Troyanların fəaliyyəti adətən iki mərhələdən ibarət olur. Birinci mərhələdə hər hansı üsulla kompüterə göndərilmiş ziyanverici proqramı özündə saxlayan faylın kompüterə yüklənməsidir. Bu prosesə misal olaraq daxilində troyan gizlədilmiş hər hansı şəklin açılması və bu zaman həmin ziyanverici proqramın kompüterə quraşdırılmasını göstərmək olar. Növbəti mərhələdə kompüterə quraşdırılmış ziyanverici proqram sayəsində kompüterin IP ünvanı müəyyən olunur və yoluxmuş kompüter bədniyyətlilər tərəfindən idarə olunan sistemin nəzarəti altına keçir. Bundan sonra yoluxmuş kompüter, ona nəzarət edən sistem tərəfindən verilən əmrləri qəbul edir və həmin əmrlərə uyğun fəaliyyət göstərir.
- **Soxulcanlar (worms)** - ziyanverici proqramların ümumi xüsusiyyətlərini özündə əks etdirsə də, öz yayılma xüsusiyyəti ilə onlardan fərqlənir. Belə ki, viruslardan fərqli olaraq soxulcanlar özünü hər hansı fayla əlavə etməklə deyil, müstəqil şəkildə şəbəkə vasitəsi ilə yoluxur.
- **Rootkitlər** - informasiya sisteminə icazəsiz daxil olmaqla özünü gizləyən, administrator səlahiyyətlərini ələ keçirən və sistemi idarə edən ziyanvericidir.
- **Casus proqramlar** - adlanan spyware-lər kompüterə ziyan vurmur, onlar adətən məlumatları oğurlayırlar.

Ziyanverici proqramların əsas xarakterik xüsusiyyətləri gizli formada yayılması və sistemə sızması, özünü gizləməsi və istifadəçinin xəbəri olmadan kompüterə ziyan vuraraq məlumatları oğurlamasıdır.

Ziyanverici proqramlar kompüterlərə necə nüfuz edir?

Ziyanverici proqramlar kompüterlərə internet və ya hər hansı yaddaş qurğuları vasitəsilə yoluxur. Belə ki, ziyanverici proqramlar sizin kompüterinizə, e-poçt hesabınıza əlavə olunmuş müxtəlif növ fayllar vasitəsilə, eləcə də, internetdən kompüterinizə yükləmək istədiyiniz fayllar vasitəsilə yoluxa bilər. Hər hansı bir keçidə səhvən kliklədikdə və ya tanımadığınız veb sayta daxil olmaq istədikdə siz qeyri-etik məzmuna və ya ziyanverici proqrama malik veb sayta daxil ola bilərsiniz. İstifadəçilərə bir kompüterdən digərinə birbaşa fayl mübadiləsinə imkan verən (P2P) şəbəkələrdə ziyanverici proqramların kompüterlərə yoluxması və yayılması riski də çox böyükdür.

Ziyanverici proqramlar kompüterin işinə necə təsir edir?

Ümumiyyətlə kompüterin ziyanverici proqrama yoluxması əlamətləri - popup (istifadəçinin fəaliyyətindən kənar, avtomatik şəkildə açılan) pəncərələr, sistemin performansının enməsi, veb brauzerə verilən sorğuların arzuolunmaz veb saytlara yönləndirilməsi və s. ola bilər. Ziyanverici proqramlar sistemin normal funksionallığını o dərəcədə aşağı sala bilər ki, hətta sistemin öz işini dayandırmasına, məlumatların dəyişdirilməsinə səbəb ola bilər və həmçinin, şəbəkənin performasını aşağı sala bilər. Bundan başqa, bəzən kompüteri yenidən işə salmaq və ya söndürmək mümkün olmur.

Kompüterinizin ziyanverici proqramlara yoluxduğunu düşünürsünüzsə:

- Login, şifrə və digər konfidensial məlumatlardan istifadəni dayandırın. Çünki siz klaviaturadan bu məlumatları daxil etdikcə onlar bədniyyətli tərəfə ötürülə bilər.
- Dərhal şifrələrinizi dəyişin və həmin kompüterdən öz e-poçt və sosial şəbəkə hesablarınıza daxil olmayın.
- Kompüterinizin əməliyyat sistemini onlayn təhlükələrdən qorumaq üçün antivirus proqram təminatlarından istifadə edin. Antivirus proqramlarını quraşdırmaq üçün onları etibarlı mənbələrdən endirin və ya əldə edin.
- Mövcud antivirus proqramını işlək vəziyyətə gətirin. Əmin olun ki, antivirus yenilənib və o kompüterinizi müntəzəm olaraq viruslara qarşı yoxlayır.
- Tanımadığınız və ya özünüz quraşdırmadığınız proqram təminatlarının xəbərdarlıqlarına qarşı diqqətli olun. Xəbərdarlıqlarda başqa bir proqramı kompüterinizə yükləmək və quraşdırmağınız tələb oluna bilər. Bu cür

xəbərdarlılqlara misal olaraq xüsusilə kompüterinizdə virus olduğunu bildirən və təmizlənməsi üçün yalnız həmin proqramın istifadəsini tövsiyə edən mesajları misal göstərmək olar. Bu xəbərdarlıqlar çox zaman virus və ziyanverici proqramları asanlıqla sizin kompüterinizə quraşdırmaq üçün istifadə olunur.

Qurğularınızdakı proqram təminatlarını müntəzəm olaraq yeniləyin:
Kibercinaykarlar hər zaman proqramlardakı boşluqlardan bacarıqla istifadə etməyə cəhd göstərirlər. Buna görə də,

- Müntəzəm olaraq antivirus və anticasus poqram təminatlarını, əməliyyat sistemlərini, mətn prosessorlarını və digər proqramları yeniləyin;
- Proqramların avtomatik yenilənmə funksiyasını aktiv edin;
- İstifadə etmədiyiniz proqramları qurğularınızın əməliyyat sistemindən silin.

Mürəkkəb şifrələrdən istifadə edin və onları gizli saxlayın:

- Mürəkkəb şifrə - minimum 10 simvoldan ibarət olmalı, həmçinin tərkibində hərf, rəqəm və başqa simvolların birləşməsini saxlamalıdır;
- Şifrənizi başqa şəxslərlə bölüşməyin və onları İnternet vasitəsilə ötürməyin;
- Eyni şifrəni bir neçə sosial şəbəkə və ya e-poçt hesabında istifadə etməyin. Çünki şifrəniz dələduz tərəfindən ələ keçirildiyi zaman bu sizin bütün hesablarınızın oğurlanması ilə nəticələnə bilər.

Firewall-u heç vaxt deaktiv etməyin:
Firewall kompüteriniz və İnternet arasında müdafiə səddi rolunu oynayır. Onun 1 dəqiqəlik belə sönməsi kompüterin ziyanvericiyə yoluxma riskini dəfələrlə artırır.

USB yaddaş qurğularından istifadə edərkən diqqətli olun:

- Kompüterinizə naməlum USB tipli yaddaş qurğularını qoşmayın;
- USB yaddaş qurğusundakı naməlum faylları açmayın;
- USB yaddaş qurğularının kompüterə qoşulması zamanı avtomatik açılması prosesini sistemin sazlamaları bölməsindən deaktiv edin.